(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10105449 A**

(43) Date of publication of application: **24.04.98**

(51) Int. Cl **G06F 12/00**
G06F 12/14

(21) Application number: **09182245**

(22) Date of filing: **08.07.97**

(30) Priority: **29.07.96 CA 96 2182254**

(71) Applicant: **INTERNATL BUSINESS MACH CORP <IBM>**

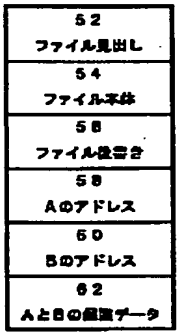
(72) Inventor: **UEIDON KOU**

(54) **METHOD FOR GENERATING PROTECTION FILE PACKAGING**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a mechanism for packing some file components by receiving various kinds of security requirments for the components irrespective of an effect whether they are a part or the whole of a file and a document or transaction.

SOLUTION: By this file format, the plural files are wrapped so as to be a single entity for storage or exchange and the security requirements being different from another file are set in the respective files. By using the protection file format, different file types are exchanged by a single wrapper and one file is divided into plural sections and wrapped to be the single file. Security protection is independently executed in respective sessions in the file so that only confidential information is protected and another session is not required to be security-protected so much. Or it is kept in a state with no necessity at all.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－105449

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/00	５３７	Ｇ０６Ｆ	12/00	５３７Ａ
	12/14	３２０		12/14	３２０Ａ

審査請求　未請求　請求項の数19　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－182245

(22)出願日　平成９年(1997)７月８日

(31)優先権主張番号　２１８２２５４

(32)優先日　1996年７月29日

(33)優先権主張国　カナダ（ＣＡ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　ウェイドン・コウ
カナダ国　Ｍ１Ｖ　３Ｐ１　オンタリオ州　スカウボロウ　クレサント　エンチャント　ヒルズ　195

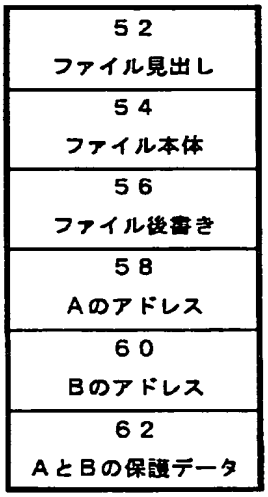
(74)代理人　弁理士　坂口　博　（外１名）

(54)【発明の名称】　保護ファイルパッケージング作成方法

(57)【要約】

【課題】　本発明の目的は、いくつかのファイルコンポーネントを、それがファイルの一部、全部、文書または取引かどうかに関わらず、これらのコンポーネントに対する多様なセキュリティ要件を受け入れ、パックするメカニズムを提供することである。

【解決手段】　このファイルフォーマットによれば、複数のファイルをラップして記憶または交換用に単一のエンティティにでき、各ファイルには、他のファイルとは異なるセキュリティ要件を設定できる。この保護ファイルフォーマットを使えば、異なるファイルタイプを単一のラッパーで交換でき、また、１つのファイルを複数のセクションに分割して、それらを単一ファイルにラップできる。ファイル内の各セクションは、独自にセキュリティ保護がなされるので、機密情報だけを保護し、他のセクションはセキュリティ保護の必要があまりない、または全くその必要がない状態にしておくことができる。



1

【特許請求の範囲】

【請求項１】保護ファイルパッケージングの作成方法であって、

共にパッケージされるファイルコンポーネントを識別し、

前記各ファイルコンポーネントのセキュリティ要件を指定し、

前記保護ファイルパッケージングのセキュリティ要件を指定し、

前記各ファイルコンポーネントの前記セキュリティ要件のパラメータを取得し、前記各ファイルコンポーネントに関連する前記セキュリティ要件に関連のセキュリティ関数を呼び出して前記各ファイルコンポーネントを処理し、

前記保護ファイルパッケージングのセキュリティ要件のパラメータを取得し、前記保護ファイルパッケージングのセキュリティ要件のパラメータを取得して、前記保護ファイルパッケージングに関連する前記セキュリティ要件に関連のセキュリティ関数を呼び出すことを特徴とする前記方法。

【請求項２】前記各ファイルコンポーネントに必要なセキュリティ保護を識別し、前記セキュリティ保護に関連するセキュリティアルゴリズムを識別することより成る前記各ファイルのセキュリティ要件を指定するステップと、

セキュリティアルゴリズムのパラメータを取得することより成る前記各ファイルコンポーネントのセキュリティ要件のパラメータを取得するステップとを有することを特徴とする請求項１記載の方法。

【請求項３】前記各ファイルのセキュリティ要件を指定する前記ステップが、さらに前記アルゴリズムの操作モード、使用するキャラクタセットおよび出力ファイル名を指定することより成ることを特徴とする請求項２記載の方法。

【請求項４】前記ファイルコンポーネントが個々のファイルであることを特徴とする請求項１記載の方法。

【請求項５】前記ファイルコンポーネントが複合ファイルのセクションであることを特徴とする請求項１記載の方法。

【請求項６】ラッパー内にパッケージするファイルコンポーネントを選択し、

(a)ファイルデータのポインタおよび前記ファイルデータのセキュリティ保護を含む前記各ファイルコンポーネントのファイル本体と、(b)保護形式の前記ファイルデータを含む少なくとも１つのデータファイルとを提供するためのファイルコンポーネントを再フォーマットし、

前記ラッパーの始まりおよび長さを識別して前記ラッパーのファイル見出しを処理し、

前記ラッパーにセキュリティ保護を提供するファイル後書きを処理することを特徴とする一般保護ファイルラッパーの作成方法。

2

【請求項７】ラッパーを処理するステップが、さらに、(i)ファイル見出し、(ii)ファイル本体のすべて、(iii)ファイル後書きおよび(iv)前記少なくとも１つのデータファイルの順であることを特徴とする請求項６記載の方法。

【請求項８】前記各ファイル本体がさらに前記ファイルコンポーネントおよび前記ファイル本体の長さを識別するタグから成り、前記セキュリティ保護がセキュリティタイプおよび前記保護形式のファイルデータにアクセスするための前記セキュリティタイプのセキュリティアルゴリズムより成ることを特徴とする請求項６記載の方法。

【請求項９】前記ファイル後書きが前記後書きの長さおよびセキュリティ規格を識別するタグと、ラッパーのパラメータとを含むことを特徴とする請求項６記載の方法。

【請求項１０】前記ファイルコンポーネントが個々のファイルであることを特徴とする請求項６記載の方法。

【請求項１１】前記ファイルコンポーネントが複合ファイルのセクションであることを特徴とする請求項６記載の方法。

【請求項１２】ラッパーの始まりおよび長さを識別するための見出しと、

ファイルデータのポインタ、前記ファイルデータのためのセキュリティ規格および前記ファイルデータにアクセスするための出力ファイル規格パラメータを含む少なくとも１つのファイル本体と、

前記ラッパーのセキュリティ規格を含む後書きと、

前記ファイルデータを含むデータファイルとからなる伝送または記憶のためにファイルを保護するラッパー。

【請求項１３】前記ファイルデータのうち少なくともいくつかが、暗号化、データ完全性またはデジタル署名の少なくとも１つにより保護されていることを特徴とする請求項１２記載のラッパー。

【請求項１４】前記セキュリティ規格が、セキュリティタイプ、セキュリティアルゴリズム、セキュリティアルゴリズムパラメータおよび前記セキュリティアルゴリズムのための操作モードを含んでいることを特徴とする請求項１２記載のラッパー。

【請求項１５】プレーンテキスト形式のアドレスデータをさらに含むことを特徴とする請求項１２記載のラッパー。

【請求項１６】前記アドレスデータが前記データファイル内の少なくとも１つの初期データセグメントに含まれることを特徴とする請求項１５記載のラッパー。

【請求項１７】前記アドレスデータが前記見出しの前に位置していることを特徴とする請求項１５記載のラッパー。

【請求項１８】保護ファイルパッケージングを作成する

方法ステップを実施するためにマシンに実行可能な命令のプログラムを実現する、前記マシンに読み取り可能なプログラム記憶デバイスにおいて、前記方法ステップが、

共にパッケージされるファイルコンポーネントを識別し、

前記各ファイルコンポーネントのセキュリティ要件を指定し、

保護ファイルパッケージングのセキュリティ要件を指定し、

前記各ファイルコンポーネントの前記セキュリティ要件のパラメータを取得し、前記各ファイルコンポーネントに関連する前記セキュリティ要件に関連のセキュリティ関数を呼び出して前記各ファイルコンポーネントを処理し、

前記保護ファイルパッケージングのセキュリティ要件のパラメータを取得し、前記保護ファイルパッケージングのセキュリティ要件のパラメータを取得して、前記保護ファイルパッケージングに関連する前記セキュリティ要件に関連のセキュリティ関数を呼び出すことより成ることを特徴とするプログラム記憶デバイス。

【請求項１９】一般保護ファイルラッパーを作成する方法ステップを実施するためにマシンに実行可能な命令のプログラムを実現する、前記マシンに読み取り可能なプログラム記憶デバイスにおいて、前記方法ステップが、

ラッパー内にパッケージするファイルコンポーネントを選択し、

(a)ファイルデータのポインタおよび前記ファイルデータのセキュリティ保護を含む前記各ファイルコンポーネントのファイル本体と、(b)保護形式の前記ファイルデータを含む少なくとも１つのデータファイルを提供するためにファイルコンポーネントを再フォーマットし、

前記ラッパーの始まりおよび長さを識別して前記ラッパーのファイル見出しを処理し、

前記ラッパーにセキュリティ保護を提供するファイル後書きを処理することより成ることを特徴とするプログラム記憶デバイス。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子データ伝送の分野に関わり、異なるセキュリティ要件を有する複数のデータコンポーネントの記憶または伝送を安全にバンドル操作することのできるファイル構造を提供するものである。このファイル構造を勝手に書き換えるようなことがあると、即時に中継ぎコンポーネントが開かれてそれが明らかとなる。

【０００２】

【従来の技術】情報の電子記憶および伝送は、商取引に多く使われつつある。商業情報は、異なるソースから入力されたデータが含まれるため非常に複雑であり、しかも、有意な文書またはつながりのある文書とするために、ひとまとめにする必要がある。また、このデータの中には、取り扱いにあまり注意を要さない、または全く注意する必要のない情報に紛れて、財務データなど、取り扱いに非常に慎重を要する情報がある。

【０００３】この種の電子情報は、例えば、複数の分離電子ファイルまたは文書として、複数のセクションまたはデータフィールドを有する単一電子ファイル（複合ファイル）の形式、または複数の複合電子ファイルの組み合わせなど様々な方式で維持される。

【０００４】取り扱いに慎重を要する度合いに応じて、電子情報の異なる部分は、情報を見るか、または情報を修正あるいは変更する際に認可されていないアクセスを防止するために、様々な形式のセキュリティ保護を必要とする。

【０００５】完全なファイル一貫性を備えた保護ファイルフォーマットを実施することが、データ記憶システムの要件として長く認識されてきている。このようなシステムにおいては、フィッシャーの米国特許第5,475,826号「単一ハッシュを用いた揮発性ファイルの保護方法」に記載されているように、すべての記録間の内部関係は、一般に単一ファイルハッシュ値で維持されまとめられている。

【０００６】タリジェント社の米国特許第5,504,892号「拡張可能オブジェクト指向ファイルシステム」は、オブジェクト指向プログラミングの階層性を利用して、ボリューム、ディレクトリおよびファイルサブクラスへと下位に分類されたファイルシステムエントリクラスを備えた拡張可能オブジェクト指向ファイルシステムにフレームワークを提供するシステムの実施例を開示している。ユーザ確認および保護ドメインを、ファイルシステムエンティティへの認可されていないアクセスから守るために用いている。ユーザ確認は、ローカル確認サービスを提供することによってなされ、保護ドメインは、ファイルシステムエンティティのうちの１つの方法によって実施される。他管轄ファイルシステムと常時情報交換できるようにするために、該特許に開示されているシステムへ他管轄ファイルシステムを移す前に、他管轄ファイルを互換性のあるフォーマットにパッケージングできるようそのメカニズムが公開されている。またそれを元の他管轄ファイルシステムへ戻すときは、ファイル類は他管轄ファイルシステムのフォーマットにアンパッケージングされる。

【０００７】ハネウエル社の米国特許第4,713,753号「フォーマットコントロールによる安全なデータプロセッシングシステムアーキテクチャ」は、ファイルフォーマットコントロールおよび保護ファイルシステムを用いた、データの安全な記憶およびプロセッシングのための別のデータプロセッシングシステムアーキテクチャを示している。この方法では、保護システムファイル類は、

常に安全なプロセッサ内にあり、そのファイル類へのユーザアクセスは、該ファイル類に関連のあるフォーマットと、各ファイルの属性の関数または要求された操作を行うサブシステムとの比較の関数として提供されている。

【０００８】欧州特許出願番号EP661651-A1号は、ディレクトリサービスをファイルシステムサービスと統合し、ディレクトリエントリおよびその他のファイル類を共通の論理フォーマットでストアすることを開示している。このシステムによれば、共通のツールセットを、エンティティと、利用する共通のネームスペースとの両方で操作することができる。ディレクトリサービスエントリへの認可されていないアクセスを防止するためにセキュリティの手段を講じている。

【０００９】ＩＢＭの技術公開定期刊行物に記載された「データベースセキュリティ／認可メカニズム」（Vol. 28, No.3、1985年8月）および「共有ファイル用の変更通知サービス」（Vol.36, No.8、1993年8月）には、ファイルフォーマット付きのファイルメンテナンスユーティリティを含むデータベースのセキュリティおよび認可メカニズムが示されている。

【００１０】電子商業用途において、取引中の財務データには暗号を必要とするものもあれば、データ完全性（読み込み専用アクセス）を必要とするその他の情報もあり、さらに取引全体またはその一部にはデジタル署名を必要とするものもある。取引には、通信ソフトにわかる形式のプレーンテキスト形式の宛名情報も含まれる。最も慎重な取り扱いを要する情報を保護するために、全体の取引ファイルを簡単に暗号化することはできない。というのは、これをすると、通信宛名情報を通信ソフトウェアに読み込み不可能な形式に変換してしまうためである。

【００１１】ファイルの一部のみの暗号化は、いくつかのタイプのファイルで既に実施されている。例えば、表計算の特定のセルだけを暗号化することのできる暗号アルゴリズムがある。しかし、この技術は、広範なファイルフォーマットや電子伝送用ファイルには利用できない。また、ファイル内の暗号化された部分を、ファイルのその部分または他の部分の如何に関わらず、他のセキュリティ要件と組み合わせることができない。

【００１２】電子顧客による単純な購買行為は、複数のセキュリティ保護を必要とする単一複合文書を包含する取引の一例である。各取引ファイルには、複数のデータフィールドが含まれ、各データフィールドには、同取引において他のフィールドとは異なるセキュリティ要件がある。例えば、クレジットカード番号やカード期限といったデータには暗号化が必要であり、宛名情報はデータの完全性が必要であり、さらに取引全体にはデジタル署名が必要である。

【００１３】同様に、実際の取引では、売り手と買い手

が標準形式の下で交渉する。その形式で印刷された情報の多くはセキュリティ保護を必要としない。しかし、特にオファーが、安全でないネットワークを通して行われる場合には、価格は秘密であり、暗号化が必要な場合もある。カウンターオファーによって条件は取り消されたり、さらに追加される可能性があるため、オファーに付けられた条件にも暗号化が必要であるが、暗号化された情報は、次の伝送時にはその大きさが異なる可能性がある。さらに、交渉の最中に一方の当事者により変更がなされると、変更を行った当事者が署名する（最初に戻る）必要がある。

【００１４】他のタイプの商業用途として、例えば、２人以上の人間により準備された取引に際しての電子文書化から生じた、または２つ以上のソースから生じた複数のファイルまたは文書が挙げられる。政府機関との典型的な商取引には、背景文書の他、最終注文書が含まれる。他の商取引を例に挙げると、見積書、見積依頼書、入札、入札依頼書、送り状および受領書がある。

【００１５】１回の取引に複数の文書が関わってくるため、すべてのファイルを一緒に伝送または記録のためにパッケージしなければならない。しかし、パッケージ内の各ファイルは、取引で使用する他のファイルに必要とされるセキュリティのタイプからは独立した別個のセキュリティ要件を有しているため、これらの用途での交換または記憶には、複数のファイルを、複数のセキュリティ要件を有する単一のエンティティとしてラップする必要がある。

【００１６】伝送または記憶のために、複数のファイルを単一ファイルにパックするのに現在使用できるいくつかのユーティリティプログラムがある（例えば、PCではPKZIP、UNIXではtar）。また、複数のファイル記録間でデータ交換を提供するメカニズムもある。例えば、ワンラボラトリ社の米国特許第5,021,995号「データ交換装置および方法」は、ソースファイル論理記録内のフィールドをマークするのに使われるデータを示すための一般形式を生成することによるファイル記録間のデータ交換を開示しており、インダストリーテクノロジーリサーチインスティテュート社の米国特許第5,522,066号「異なるファイルシステムフォーマットにストアされた複数の記録にアクセスするためのインターフェース」は、異なるファイルシステムフォーマットにストアされた複数の記録にアクセスするためのインターフェースを開示している。しかし、このどれもが、いったん多くのファイルまたは記録にアクセスしたり、これらを一緒にパックしてしまうと、個々のファイルまたは記録に関連する異なるセキュリティ機能を維持することのできる手段を提供していない。

【００１７】

【発明が解決しようとする課題】本発明の目的は、いくつかのファイルコンポーネントを、それがファイルの一

部、フルファイル、文書または取引かどうかに関わらず、これらのコンポーネントに対する多様なセキュリティ要件を受け入れ、パックするメカニズムを提供することである。

【００１８】本発明の他の目的は、操作環境から独立していて、あらゆる種類のファイルに使用可能なパッキングメカニズムを提供することである。

【００１９】

【課題を解決するための手段】従って、本発明は、一緒にパッケージされるファイルコンポーネントを識別し、各ファイルコンポーネントに対してセキュリティパラメータを指定し、安全なファイルパッケージングに必要なセキュリティ要件を指定するステップを含む安全なファイルパッケージングを作成する方法を提供するものである。そして、各ファイルコンポーネントに対して、セキュリティ要件のパラメータを取得すると、セキュリティ要件と関連したセキュリティ関数が呼び出され、コンポーネントが処理される。さらに、安全なファイルパッケージングのために、セキュリティ要件のパラメータを取得すると、これらのセキュリティ要件と関連したセキュリティ関数が呼び出される。

【００２０】各ファイルのセキュリティ要件が指定されたら、必要なセキュリティ保護および関連のセキュリティアルゴリズムが指定されることが好ましい。

【００２１】本発明の他の態様によれば、ラッパーにパッケージされるファイルコンポーネントを選択し、各ファイルコンポーネントおよびファイルデータを含む少なくとも１つのファイルにファイル本体を提供するためにファイルコンポーネントを再フォーマットすることよりなる一般の安全なファイルラッパー（ｆｉｌｅ　ｗｒａｐｐｅｒ）を作成する方法を提供するものである。ファイル本体には、ファイルデータおよびセキュリティ保護に対するポインタが含まれ、さらにファイルコンポーネントおよびファイルの長さを識別するタグが含まれていることが好ましい。また、セキュリティ保護には、保護されるファイルデータにアクセスするために、セキュリティタイプおよびそれに関連するアルゴリズムが含まれていることが好ましい。

【００２２】また、この方法にはラッパーの始まりと長さを識別するラッパーのファイル見出しを処理し、ラッパーにセキュリティ保護を提供するファイル後書きを処理するステップが含まれる。

【００２３】本発明のさらに他の態様によれば、ラッパーの始まりと長さを識別する見出し、ファイルデータに対するポインタを含む少なくとも１つのファイル本体、ファイルデータ用保護規格およびファイルデータにアクセスするための出力ファイル規格パラメータ、ラッパー用の保護規格を含む後書き、およびファイルデータを含むファイルを有する伝送または記憶のための保護ファイル用ラッパーを提供するものである。

【００２４】本発明はまた、上述した方法ステップを実施するための、マシンに実行できるプログラム命令を実現する、マシンに読出し可能なプログラム記憶デバイスにも適用できる。

【００２５】

【発明の実施の形態】図１に、商品を供給する際の入札などの電子取引に使われる典型的な通信ファイルの構造を示す。このファイルには、複数のフィールドがあり、各フィールドには、取引に必要な重要な情報が含まれている。フィールド１には、伝送のためのアドレス宛先がある。上述したとおり、このアドレスは、通常プレーンテキストにフォーマットされており、伝送中にネットワークを通じて利用される標準の通信ソフトウェアに簡単に理解できるようになっている。しかし、アドレスフィールド１は、データが有効アドレスを確実に記述するよう、伝送の前に完全性チェックも受けるようになっている。

【００２６】フィールド２には、売り主からのセット価格といったような発注情報がある。この情報には特定顧客に対してのみのディスカウントが含まれる可能性があるため、このフィールドは、その受信者だけがこの情報にアクセスできるよう暗号化されることがある。

【００２７】フィールド３、４および５には、配送日やその他販売条件といった機密性の低い情報がある。この情報は、暗号化を必要とするほど取り扱いに慎重を要するようなものではないが、それでも、ファイルハッシュなど、他のセキュリティ手段を講じて受信者のみにアクセスを制限する必要がある。

【００２８】最後に、フィールド６には、入札者が受信者により受け入れられたときにデジタル的に「署名を戻す」必要のある入札当事者のデジタル署名がある。

【００２９】図１の入札文書は、単独の取引ファイルにもできるし、大きな取引を構成する多数の文書の内の１つとすることもできる。図１の文書が、例えば、専売製造プロセスを実行するシステムソフトウェアの供給に関係する場合には、取引を形成する他の文書と一緒に伝送する際に、価格約款の暗号化に加え、ソフトウェア仕様書およびそのソフトウェアのソースでさえも、ファイル全体を安全にラップする必要のある機密度の高い情報である。

【００３０】従って、これらの異なるセキュリティ要件に対処するために、本発明は、図２の一実施例に示す一般保護ファイルフォーマット（GSFF）を提供する。このファイルフォーマットによれば、複数のファイルをラップして記憶または交換用に単一のエンティティにすることができる。各ファイルには、他のファイルとは異なるセキュリティ要件を設定することができる。この保護ファイルフォーマットを使えば、異なるファイルタイプを単一のラッパーで交換することができる。また、この保護ファイルフォーマットによれば、１つのファイルを複

数のセクションに分割して、それらを単一ファイルにラップすることができる。ファイル内の各セクションは、独自にセキュリティ保護がなされる。これによって、機密情報だけを保護し、他のセクションはセキュリティ保護の必要があまりない、または全くその必要がない状態にしておくことができる。その結果、セキュリティに関与する操作は、ファイルのほんの一部しか必要ないため、性能が上がる。

【００３１】本発明の一般保護ファイルフォーマットがサポートするセキュリティ機能には、暗号化によるデータ機密性、ハッシュによるデータ完全性、メッセージダイジェスト、メッセージ確認コード（MAC、ANSI規格として定義されている）およびデジタル署名が含まれる。

【００３２】図２に示すように、一般保護ファイルフォーマットには、ファイル見出し１０、続いて、複数のファイル本体１２、ファイル後書き１４、その次にデータ１６がある。各ファイル本体１２には、後述するとおり、他の実施される本体とは異なるセキュリティ要件を設定することができる。例えば、１つのファイルは暗号化を必要とし、他のファイルはデータ完全性の保護だけを必要とする場合などである。

【００３３】各ファイルは、その要件に従ってラップされ、ファイル本体に記述される。データのポインタは、ファイル本体セクションに含まれ、データはファイル後書きの後に置かれる。

【００３４】本発明の一般保護ファイルフォーマットはディレクトリベースのファイルフォーマットである。ファイル見出し、ファイル本体およびファイル後書きはラッパー内ではディレクトリとみなされる。ファイル見出しには、一般保護ファイルフォーマットのファイル識別子、バージョン番号およびラッパーの長さが含まれる。各ファイル本体には、そのファイル本体に関連するエントリが含まれる。ファイル後書きは、ラッパー全体のセキュリティ保護に用いることができる。

【００３５】ファイル見出しの構造の概略を図３に示す。ファイル見出しには、一般保護ファイルフォーマット識別子２０、ファイルフォーマットを単に識別する一対のバイトのタグ（例えば、インテルとモトローラのバイト順を識別する）、一般保護ファイルフォーマットのバージョン番号２２、ファイルインジケータ２４および一般保護ファイルフォーマットの全ファイル長２６が含まれる。

【００３６】各ファイル本体は、ラッパーに含まれるファイルを記述する。図４に概略を示すように、ファイル本体には、本体ファイルとしてファイルのタイプを識別して、ファイル長を設定するためのファイル本体タグ２８、次にセキュリティ規格３０がある。セキュリティ規格には、セキュリティタイプ、セキュリティアルゴリズム、セキュリティアルゴリズムパラメータ、暗号鍵情報、操作モード、フィルタ、キャラクタセット、出力ファイル規格パラメータ、データ長、およびフィルタ後書きに後続する安全に保護されたファイルデータ用データポインタが含まれている。

【００３７】図５にその概略を示すファイル後書きには、ファイルを後書きとして識別し、後書きファイルの長さを指定するファイル後書きタグ３２がある。後書きファイルにはまた、セキュリティ規格およびパラメータを設定するセクション３４も含まれている。セキュリティ規格を含むバイトは、セキュリティタイプ、セキュリティアルゴリズム、セキュリティアルゴリズムパラメータ、暗号鍵情報、操作モード、フィルタ、キャラクタセットその他セキュリティパラメータを指定する。

【００３８】図６に、本発明の一般保護ファイルフォーマットの伝送目的のための変形例を示す。本実施例において、プレーンテキスト形式のアドレス４２は、第１のデータセグメントであり、その後に追加データ（４４および４８）用の追加データセグメント、暗号化データ４６、およびデジタル署名データ５０が続く。GSFFファイル見出し、ファイル本体、およびファイル後書きの長さは既知であるため、アドレスデータは即時に位置づけされ、通信目的に用いることができる。

【００３９】アドレスデータはまた、GSFFファイルから抽出され、図７に示すフォーマットで通信に用いることができる。アドレス５１Ａは、ラップされたファイルまたはファイルの集合の先頭になる。両実施例とも多数の文書をセキュリティ要件付きで単一のアドレスへ伝送するのに有益である。

【００４０】図８および９に、データを複数の宛先に伝送する２つの変形例を示す。図８において、複数アドレス５８および６０が、最初の２つのデータセグメントとしてGSFFファイル内に含まれている。保護データセグメント６２は、これら２つのアドレスへ送られる。図９において、GSFFファイルには、複数のデータセグメントおよび複数のアドレスが含まれる。各アドレスに、異なるデータセグメントが送られる。

【００４１】図６、７、８および９に示したすべてのケースについて、通信ソフトウェアは、保護データを伝送するにあたってGSFFファイルのデータ完全性を壊すことなく、アドレス情報を簡単に位置づけ、抽出し、使用することができる。GSFFファイルに含まれる保護データを伝送する際に、暗号化もデジタル署名確認も必要とされない。

【００４２】本発明はまた、様々なファイルに対するセキリュティを与える方法も提供する。図１０および１１にそのフロー図を示す。

【００４３】図１０に、単一複合ファイルまたは多数のファイルを、一般保護ファイルフォーマット（GSFF）で「ラップ」するステップを示す。

【００４４】好ましい実施形態によれば、第１のステップは、ファイル（複数のファイルをラップする場合）ま

たは処理するファイルのセクション（単一ファイルをラップする場合）を識別することである（ブロック７８）。各ファイル（またはファイルのセクション）に対するセキュリティ要件を指定する必要がある（ブロック８０）。このステップでは、各ファイル（またはファイルのセクション）が必要とするセキュリティ保護項目は何か、また、各セキュリティ保護のためのセキュリティアルゴリズム、適用可能であれば選択したアルゴリズムの操作モード、フィルタ要件、用いるキャラクタセット、出力ファイル名およびその他情報を識別する。同様に、GSFFファイル全体のセキュリティ要件を指定する必要がある（ブロック８２）。セキュリティ要件を識別後、各セキュリティアルゴリズムに用いるパラメータを取得し、各ファイル（またはファイルのセクション）を処理する（ブロック８４）。GSFFファイル全体に必要なセキュリティアルゴリズムのパラメータを取得後、各セキュリティアルゴリズムの関連セキュリティ関数を呼び出し、GSFFファイルを作成する（ブロック８６）。

【００４５】図１１に、受信に際して一般保護ファイルフォーマットファイルを「アンラップ」するためのステップを示す。「アンラップ」プロセスは、ファイルを開き（ブロック８８）、GSFFファイル識別子をチェックする（ブロック８９）から始まる。開いたファイルがGSFFファイルの場合には、プロセスはそのまま進み、そうでない場合には停止する。GSFFファイルのバージョン、ファイルインジケータおよびファイル長を判断するためにGSFFファイル見出しが処理される（ブロック９０）。各ファイル本体およびファイル後書き情報が読み込まれ、GSFFファイル全体および各ファイル（またはファイルの各セクション）のセキュリティ保護タイプが判断される（ブロック９２）。GSFFファイル全体のセキュリティ関数が呼び出される（ブロック９４）。セキュリティ関数の一例として、全GSFFのデジタル確認関数がある。次に、各ファイル（またはファイルの各セクション）のセキュリティ関数が呼び出される（ブロック９６）。ラップされたファイルが複数の場合には、出力データが複数のファイルに書き込まれ、ラップされた複合ファイルの場合には、出力データが単一のファイルに書き込まれる（ブロック９８）。GSFFファイルは閉じられ、「アンラップ」プロセスが終了する（ブロック１００）。

【００４６】上記に提案した解決策は、操作環境からは独立しており、いかなるファイルタイプでも動作するものであるため、ユーザは、複合文書またはファイルパッケージ内の単一ファイルの一部分の暗号化および／またはデジタル署名を行うことができる。各文書／ファイルは、複数のセキュリティ要件を有する１つのエンティティとして扱われる。一般保護ファイルフォーマット（GSFF）の単一ファイルまたはラップされたファイルの集合体は、異なる操作環境で自由に交換することができる。

【００４７】本発明の好ましい実施形態について説明してきたが、当業者にとって明白な変更は、特許請求の範囲に含まれるものとする。

【００４８】まとめとして、本発明の構成に関して以下の事項を開示する。

（１）保護ファイルパッケージングの作成方法であって、共にパッケージされるファイルコンポーネントを識別し、前記各ファイルコンポーネントのセキュリティ要件を指定し、前記保護ファイルパッケージングのセキュリティ要件を指定し、前記各ファイルコンポーネントの前記セキュリティ要件のパラメータを取得し、前記各ファイルコンポーネントに関連する前記セキュリティ要件に関連のセキュリティ関数を呼び出して前記各ファイルコンポーネントを処理し、前記保護ファイルパッケージングのセキュリティ要件のパラメータを取得し、前記保護ファイルパッケージングのセキュリティ要件のパラメータを取得して、前記保護ファイルパッケージングに関連する前記セキュリティ要件に関連のセキュリティ関数を呼び出すことを特徴とする前記方法。

（２）前記各ファイルコンポーネントに必要なセキュリティ保護を識別し、前記セキュリティ保護に関連するセキュリティアルゴリズムを識別することより成る前記各ファイルのセキュリティ要件を指定するステップと、セキュリティアルゴリズムのパラメータを取得することより成る前記各ファイルコンポーネントのセキュリティ要件のパラメータを取得するステップとを有することを特徴とする上記（１）記載の方法。

（３）前記各ファイルのセキュリティ要件を指定する前記ステップが、さらに前記アルゴリズムの操作モード、使用するキャラクタセットおよび出力ファイル名を指定することより成ることを特徴とする上記（２）記載の方法。

（４）前記ファイルコンポーネントが個々のファイルであることを特徴とする上記（１）記載の方法。

（５）前記ファイルコンポーネントが複合ファイルのセクションであることを特徴とする上記（１）記載の方法。

（６）ラッパー内にパッケージするファイルコンポーネントを選択し、(a)ファイルデータのポインタおよび前記ファイルデータのセキュリティ保護を含む前記各ファイルコンポーネントのファイル本体と、(b)保護形式の前記ファイルデータを含む少なくとも１つのデータファイルとを提供するためのファイルコンポーネントを再フォーマットし、前記ラッパーの始まりおよび長さを識別して前記ラッパーのファイル見出しを処理し、前記ラッパーにセキュリティ保護を提供するファイル後書きを処理することを特徴とする一般保護ファイルラッパーの作成方法。

（７）ラッパーを処理するステップが、さらに、(i)ファイル見出し、(ii)ファイル本体のすべて、(iii)ファイル後書きおよび(iv)前記少なくとも１つのデータファ

イルの順であることを特徴とする上記（６）記載の方法。

（８）前記各ファイル本体がさらに前記ファイルコンポーネントおよび前記ファイル本体の長さを識別するタグから成り、前記セキュリティ保護がセキュリティタイプおよび前記保護形式のファイルデータにアクセスするための前記セキュリティタイプのセキュリティアルゴリズムより成ることを特徴とする上記（６）記載の方法。

（９）前記ファイル後書きが前記後書きの長さおよびセキュリティ規格を識別するタグと、ラッパーのパラメータとを含むことを特徴とする上記（６）記載の方法。

（１０）前記ファイルコンポーネントが個々のファイルであることを特徴とする上記（６）記載の方法。

（１１）前記ファイルコンポーネントが複合ファイルのセクションであることを特徴とする上記（６）記載の方法。

（１２）ラッパーの始まりおよび長さを識別するための見出しと、ファイルデータのポインタ、前記ファイルデータのためのセキュリティ規格および前記ファイルデータにアクセスするための出力ファイル規格パラメータを含む少なくとも１つのファイル本体と、前記ラッパーのセキュリティ規格を含む後書きと、前記ファイルデータを含むデータファイルとからなる伝送または記憶のためにファイルを保護するラッパー。

（１３）前記ファイルデータのうち少なくともいくつかが、暗号化、データ完全性またはデジタル署名の少なくとも１つにより保護されていることを特徴とする上記（１２）記載のラッパー。

（１４）前記セキュリティ規格が、セキュリティタイプ、セキュリティアルゴリズム、セキュリティアルゴリズムパラメータおよび前記セキュリティアルゴリズムのための操作モードを含んでいることを特徴とする上記（１２）記載のラッパー。

（１５）プレーンテキスト形式のアドレスデータをさらに含むことを特徴とする上記（１２）記載のラッパー。

（１６）前記アドレスデータが前記データファイル内の少なくとも１つの初期データセグメントに含まれることを特徴とする上記（１５）記載のラッパー。

（１７）前記アドレスデータが前記見出しの前に位置していることを特徴とする上記（１５）記載のラッパー。

（１８）保護ファイルパッケージングを作成する方法ステップを実施するためにマシンに実行可能な命令のプログラムを実現する、前記マシンに読み取り可能なプログラム記憶デバイスにおいて、前記方法ステップが、共にパッケージされるファイルコンポーネントを識別し、前記各ファイルコンポーネントのセキュリティ要件を指定し、保護ファイルパッケージングのセキュリティ要件を指定し、前記各ファイルコンポーネントの前記セキュリティ要件のパラメータを取得し、前記各ファイルコンポーネントに関連する前記セキュリティ要件に関連のセキュリティ関数を呼び出して前記各ファイルコンポーネントを処理し、前記保護ファイルパッケージングのセキュリティ要件のパラメータを取得し、前記保護ファイルパッケージングのセキュリティ要件のパラメータを取得して、前記保護ファイルパッケージングに関連する前記セキュリティ要件に関連のセキュリティ関数を呼び出すことより成ることを特徴とするプログラム記憶デバイス。

（１９）一般保護ファイルラッパーを作成する方法ステップを実施するためにマシンに実行可能な命令のプログラムを実現する、前記マシンに読み取り可能なプログラム記憶デバイスにおいて、前記方法ステップが、ラッパー内にパッケージするファイルコンポーネントを選択し、(a)ファイルデータのポインタおよび前記ファイルデータのセキュリティ保護を含む前記各ファイルコンポーネントのファイル本体と、(b)保護形式の前記ファイルデータを含む少なくとも１つのデータファイルを提供するためにファイルコンポーネントを再フォーマットし、前記ラッパーの始まりおよび長さを識別して前記ラッパーのファイル見出しを処理し、前記ラッパーにセキュリティ保護を提供するファイル後書きを処理することより成ることを特徴とするプログラム記憶デバイス。

【図面の簡単な説明】

【図１】従来例の通信ファイルの概略図。

【図２】本発明のファイル構造の概略図。

【図３】本発明による図２のファイル構造におけるファイル見出し、ファイル本体およびファイル後書き部分の概略図。

【図４】本発明による図２のファイル構造におけるファイル見出し、ファイル本体およびファイル後書き部分の概略図。

【図５】本発明による図２のファイル構造におけるファイル見出し、ファイル本体およびファイル後書き部分の概略図。

【図６】本発明の他の態様による図２のファイル構造の変形例。

【図７】通信目的で抽出されたアドレス見出しのあるGSFFファイル。

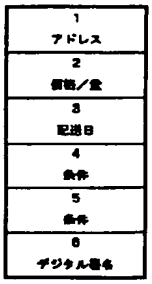
【図８】本発明の他の態様による図２のファイル構造の変形例。

【図９】本発明の他の態様による図２のファイル構造の変形例。

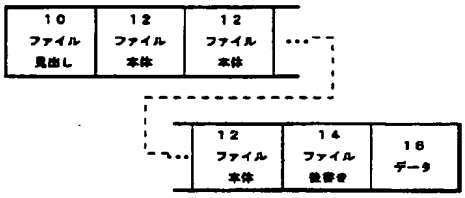
【図１０】伝送または記憶に際して、一般保護ファイルフォーマットの様々なファイルをラップするために本発明のさらに他の態様により実施されるステップのフロー図。

【図１１】伝送または記憶に際して、一般保護ファイルフォーマットの様々なファイルをアンラップするために本発明のさらに他の態様により実施されるステップのフロー図。

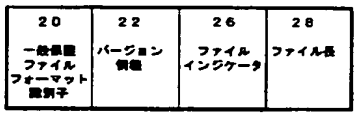
【図１】



【図２】



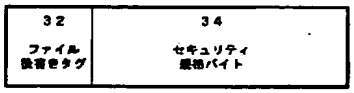
【図３】



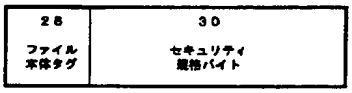
【図６】

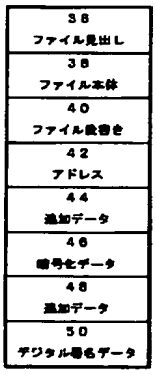
【図７】

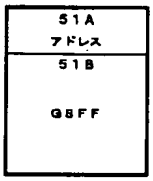
【図５】



【図４】

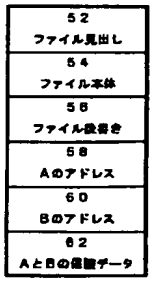


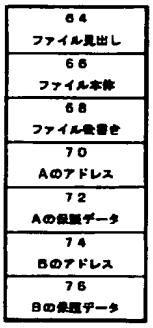




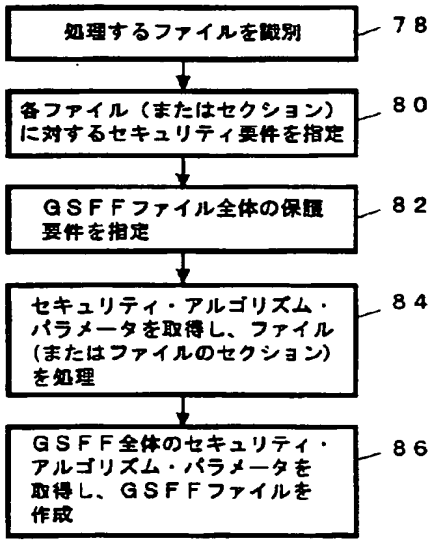
【図８】

【図９】

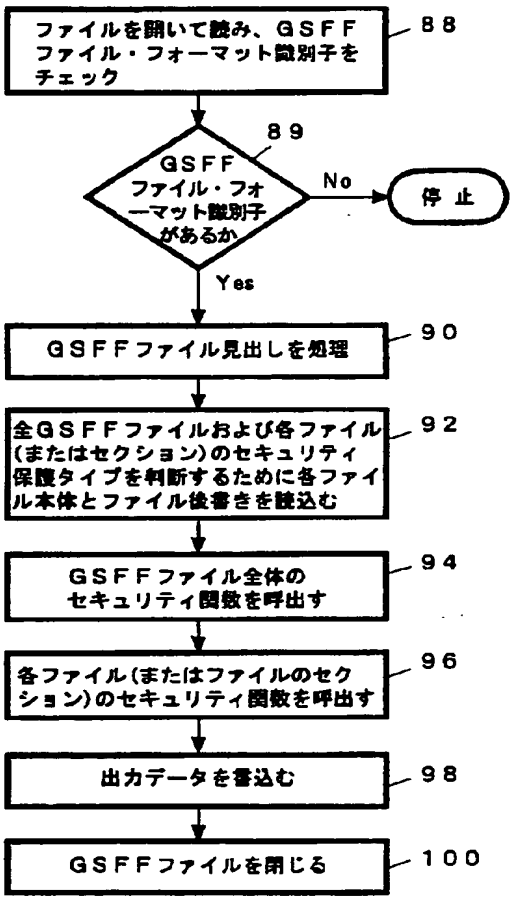




【図１０】



【図１１】


ファイルを開いて読み、ＧＳＦＦファイル・フォーマット識別子をチェック
88
GSFFファイル・フォーマット識別子があるか
89
No
停止
Yes
ＧＳＦＦファイル見出しを処理
90
全ＧＳＦＦファイルおよび各ファイル(またはセクション)のセキュリティ保護タイプを判断するために各ファイル本体とファイル後書きを読込む
92
ＧＳＦＦファイル全体のセキュリティ関数を呼出す
94
各ファイル(またはファイルのセクション)のセキュリティ関数を呼出す
96
出力データを書込む
98
ＧＳＦＦファイルを閉じる
100